Anonymous Network Coding Against Active Adversary

Oksana Trushina

Moscow Institute of Physics and Technology

2016
Outlines

1. Anonymous Transmission
2. Network Model
3. Adversary Model
4. Anonymous Scheme Requirements
5. Coset Coding
   5.1 Error Free Case
   5.2 Noisy Coding
   5.3 Explicit Error Correcting Scheme for Network Coding
6. Anonymous Scheme
7. Possible Attack
8. Conclusion
Anonymous Transmission

To guarantee a message forwarding to be untraceable

Are $m$ and $m'$ transfer the same information message? Is it possible to reveal the previous and next nodes of a message $m'$?
Network Model

Coherent network coding

Overlay network

Received message $Y = AX$, $X \in \mathbb{F}_{q^m}^n$ – sent message, $X = (x_1 \ x_2 \ \ldots \ x_n)^T$, $x_i \in \mathbb{F}_{q^m}$ rank $A = n$, $A$ – known transfer matrix over $\mathbb{F}_q$

Every relay node can decode a message from previous one
Adversary Model

External active adversary

- injects up to $t$ malicious packets: $\mathcal{Y} = A\mathcal{X} + D\mathcal{Z}$, $\mathcal{Z} \in \mathbb{F}_{q^m}^t$ – malicious packets, $D$ – transfer matrix of malicious packets
- eavesdrops up to $\mu$ packets: $\mathcal{W} = E\mathcal{Y}$, $\text{rank} E = \mu$, $E$ defines which coordinates of $\mathcal{Y}$ are eavesdropped by an adversary

Active adversary harming = passive adversary harming + erroneous transmission
Anonymous Scheme Requirements

1. Security condition. $S \in \mathbb{F}_q^m \rightarrow \mathcal{X} \in \mathbb{F}_q^n : I(S; \mathcal{W}) = 0$, necessary to prevent traceability.

2. Reliability condition. $\mathcal{Y} = A\mathcal{X} + D\mathcal{Z}$ must satisfy $H(S|\mathcal{Y}) = 0$ $\forall A \text{ rank } A = n$, $\forall D, \mathcal{Z}$.

3. Anonymous condition.

$$I(\mathcal{W}_{in} ; \mathcal{W}_{out}) = 0$$ which leads to

$$I(\mathcal{Y}_{in} ; \mathcal{Y}_{out}) = 0$$
Coset Coding. Error Free Case

\((n, n - k)\) code \(C\)

\(\sigma : \mathcal{M} \rightarrow \{C + v\}\)

\(x = \sigma(m)\)

\(x\) – concatenation of secret message \(s\) and random bits, \(s\) labels a coset, random bits decide a random point inside the coset

adversary information \(z = \mu\) coordinates of \(x\)

\[H(s|z) = \begin{cases} 
  n - \mu, & n - d + 1 \leq \mu \leq n, d - C \text{ minimal distance} \\
  k, & 0 \leq \mu \leq d' - 1, d' - C^\perp \text{ minimal distance}
\end{cases}\]

if \(C\) is MDS code, then \(k\) bits may be transmitted in secret under \(\mu \leq n - k\) observations
Coset Coding. Noisy Coding

\[ C_2 \subset C_1 \]
\[ \{(n, k_1), (n, k_2)\}, \ k_1 > k_2 \]
\[ \sigma : \mathcal{M} \to \{C_2 + \nu\} \]

\[ H_2 = \begin{pmatrix} H_1 \\ \Delta H \end{pmatrix} \]
\[ s_1 = H_1 x \]
\[ s_2 = H_2 x \]
\[ \Delta s = \Delta H x \text{ relative syndrome} \]
\[ s_2 = \begin{pmatrix} s_1 \\ \Delta s \end{pmatrix} \]

If \( x \in C_1 \) then \[ s_2 = \begin{pmatrix} 0 \\ \Delta s \end{pmatrix} \] \( C_1 \) may be filled in \( 2^{k_1 - k_2} \) cosets of \( C_2 \) by varying \( \Delta s \) given \( s_1 \equiv 0 \)
Explicit Error Correcting Coset Coding Scheme

Silva-Kschischang Scheme

\[ S \in \mathbb{F}_{q^m}^k, \ V \in \mathbb{F}_{q^m}^\mu \text{ is uniform and independent of } S \]
\[ \mathcal{U} = \begin{pmatrix} S' \\ V \end{pmatrix} \]
\[ \mathcal{X} = G_1^T \mathcal{U}, \ G_1 - \text{generator matrix of } (n, k + \mu) \text{ MRD code} \]

Error Correcting

up to \( t \) errors may be corrected if \( d_R \geq 2t + 1 \)

Security

\[ T \in \mathbb{F}_{q^m}^{n \times n}, \ T - \text{invertible matrix}, \ T^T = \begin{pmatrix} \Delta G \\ G_1 \\ G_2 \end{pmatrix} \]
\[ I(S; \mathcal{W}) = 0 \text{ if } T^T = \begin{pmatrix} \Delta G \\ \Delta G_1 \\ G_2 \end{pmatrix}, \ G_2 - \text{matrix of } (n, \mu) \text{ MRD code} \]
\[ \mathcal{X} = G_1^T \mathcal{U} = T \begin{pmatrix} 0 \\ \mathcal{U} \end{pmatrix} = T \begin{pmatrix} S' \\ V \end{pmatrix} = (\Delta G^T \Delta G_1^T G_2^T) \begin{pmatrix} S' \\ V \end{pmatrix} = (\Delta G^T \Delta G_1^T) \begin{pmatrix} 0 \\ S \end{pmatrix} + G_2^T V \]
Anonymous Scheme

Consider

\[ \chi^{\text{out}} = \chi^{\text{in}} + G_2^T \mathcal{V}' = (\Delta G^T \Delta G_1^T) \begin{pmatrix} 0 \\ S \end{pmatrix} + G_2^T (\mathcal{V} + \mathcal{V}') , \]

where \( \mathcal{V}' \) is uniform over \( \mathbb{F}_{q^m}^{\mu} \) and independent of \( \chi^{\text{in}} \).

\( \chi^{\text{out}} \) belongs to the same coset as \( \chi^{\text{in}} \) \( \Rightarrow \) transmits the same information.

Lemma

Let \( x \) and \( y \) be two independent statistical variables from finite field. If \( x \) is uniformly distributed over the field, then \( z = x + y \) is uniformly distributed as well and independent of \( y \).

Then \( \chi^{\text{out}} \) is uniform over \( \mathbb{F}_{q^m}^{\mu} \) and independent of \( \chi^{\text{in}} \).

\[ \mathcal{Y}^{\text{in}} = A_{\text{in}} \chi^{\text{in}} + D_{\text{in}} Z^{\text{in}} \]

\[ \mathcal{Y}^{\text{out}} = A_{\text{in-out}} (A_{\text{in}} (\chi^{\text{in}} + G_2^T \mathcal{V}') + D_{\text{in}} Z^{\text{in}} + D_{\text{out}} Z^{\text{out}}) \]

\[ = A_{\text{in-out}} (\mathcal{Y}^{\text{in}} + A_{\text{in}} G_2^T \mathcal{V}' + D_{\text{out}} Z^{\text{out}}) \]

\[ I(\mathcal{Y}^{\text{out}}; \mathcal{Y}^{\text{in}}) = 0 \]
Possible Attack

Eavesdrop node

\( Y^{in} \)    \( Y^{out} \)

Security condition

\( S^{in} \)    \( S^{out} \)

\( S^{in} = S^{out} \)

no

stop

\( Y^{in}, Y^{out} \) forward the same message, next hop is determined

yes

trace next node
Conclusion

The proposed scheme
+ is simple
+ doesn’t increase decoding complexity
- has requirement to network topology
Q&A